CLAIMS

What is claimed is:

1. A remote server management controller, comprising:

a web server adapted to engage in encrypted communication over a first communication link, the web server being further adapted to receive and respond to a request for secret data from a client computer over the first communication link, the secret data being adapted to encrypt a second secure communication link; and

a remote console server adapted for operable communication with the web server, the remote console server being further adapted to engage in communication with the client computer over the second communication link, wherein the remote console server receives the secret data from the web server and uses the secret data to encrypt communications sent over the second communication link.

2. The remote server management controller of claim 1 wherein the secret data is a secret key.

3. The remote server management controller of claim 1 wherein the secret data is a random number that is used by the remote console server to generate a secret key.

4. The remote server management controller of claim 2 wherein the remote console server is adapted to use the secret key to decrypt communications received over the second communication link.

5. The remote server management controller of claim 1 wherein the request for the secret data is initiated by a remote console applet executing on the client computer, the remote console applet being adapted for operable communication with a browser application executing on the client computer, the remote console applet transmitting the request for secret data to the browser application, the browser application transmitting the request for secret data to the web server via the first communication link.

6. The remote server management controller of claim 1 wherein the first communication link is between the web server and a browser application executing on the client computer.

7. The remote server management controller of claim 1wherein the second communication link is between the remote console server and a remote console applet executing on the client computer.

8. The remote server management controller of claim 1 wherein transmissions across the second communication link are encrypted using the RC4 transform.

9. A client computer, comprising:

a browser application adapted to execute on the client computer, the browser application being adapted to transmit a request for secret data to a remote server management controller across a first communication link; and

a program adapted to execute on the client computer, the program being adapted to initiate the request for secret data and use the secret data to encrypt communication over a second communication link.

10. The client computer of claim 9 wherein the secret data is a secret key.

11. The client computer of claim 9 wherein the secret data is a random number that is used by the remote console applet to generate a secret key.

12. The client computer of claim 9 wherein the program is adapted to use the secret data to decrypt information received via the second communication link.

13. The client computer of claim 9 wherein the secret data is generated by a web server in the remote server management controller.

14. The client computer of claim 9 wherein the first communication link is between a web server in the remote server management controller and the browser application.

15. The client computer of claim 9 wherein the program is a remote console applet and the second communication link is between a remote console server in the remote server management controller and the remote console applet.

16. The client computer of claim 9 wherein transmissions across the second communication link are encrypted using the RC4 transform.

17. A method of employing a first communication link between a client computer and a managed server to upgrade a second communication link between the client computer and the managed server from clear to encrypted, wherein the first communication link is encrypted, the method comprising the acts of:

receiving a request for secret data from the client computer via the first communication link;

transmitting secret data to the client computer across the first communication link responsive to the request; and

using the secret data to encrypt communications sent via the second communication link.

18. The method of claim 17 further comprising generating a secret key from the secret data.

19. The method of claim 17, further comprising using the secret data to decrypt data received via the second communication link.

20. The method of claim 17 wherein the recited acts are performed in the recited order.